

Repurposing Inexpensive Laser Welder for Laser Fault Injection

◎ **Kensho Murata**¹ Yujin Mori²

Soramichi Akiyama² Takeshi Sugawara¹

¹The University of Electro-Communications ²Ritsumeikan University

FDTC 2026, Antalya, Turkey

Contact us: kensho.murata@uec.ac.jp

Overview

Background

- Laser fault injection (LFI) is expensive, so it is limited to well-funded attackers

Prior work

- Existing low-cost setups use low-power diode lasers and require depackaging; successful attacks are limited to low-end MCUs or analog targets

Proposed method

- Repurpose an inexpensive jewelry laser welder for backside LFI on flip-chip packages without any preparation

Results

- Caused bit flips in the BRAMs of a 28 nm FPGA and recovered an AES-128 key with persistent fault analysis (PFA)

Laser Fault Injection

Laser fault injection (LFI)

- Injects faults into a target device with a focused laser
- Serious threat to cryptographic implementations

Strength

- High spatial resolution and precise timing control
 - Highly controllable faults

Weakness

- An attacker needs highly specialized equipment
 - Conventional LFI setups cost $\sim$ €150,000



Laser Station 2 © Riscure

Background: Low-Cost LFI

Low-cost LFI is an active research topic

- Cheaper setups make the attack more practical
- There are several approaches: diode lasers, 3D-printed optics and laser engravers

Work	Setup	Target	Depackaging
Kelly & Mayes (HOST 2020)	Diode laser + microscope	8-bit MCU	Mech. & chem.
Redshift (TCHES 2022)	Diode laser + microscope	Analog circuits	Mech. & chem.
RayV-Lite (Black Hat USA 2024)	Diode laser + DIY optics	—	Mech. & chem.
Courk (DEF CON 33, 2025)	Diode laser + DIY optics	32-bit MCU	Mechanical
Ours	YAG laser welder	28 nm FPGA	Not required

Low peak power limits the range of target devices; depackaging adds extra cost and effort

Key Idea: Repurposing a Laser Welder

Affordable thanks to the maker movement

- Laser engravers and welders are now widely available
- Jewelry laser welder (MW ST60x): ~\$5,000 from online retailers

Optics already built in

- Focusing optics, laser controller and monitoring camera

Laser power already high

- High-power YAG laser pulses strong enough to melt metal
- Backside illumination is possible with strong 1064 nm pulses



MW ST60x

© Maxwave

Objective and Contributions

Objective

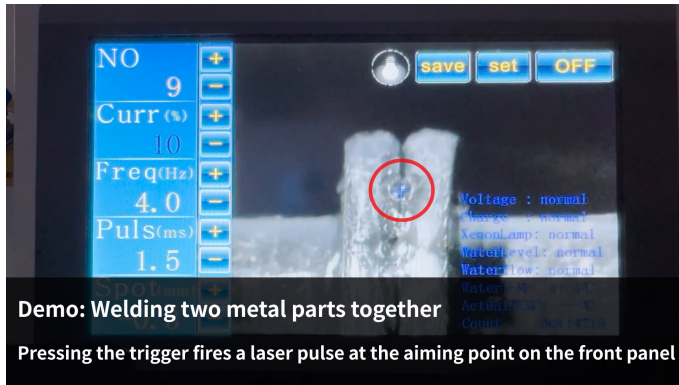
- Repurpose an inexpensive laser welder for LFI
 - Pulsed laser welder for jewelry crafting ($\sim \$5,000$)
 - Entire setup ($\sim \$6,000$): rated as standard equipment ($\leq \text{€}10,000$) under Common Criteria, not *specialized*
 - High-energy near-infrared pulses penetrate the backside silicon of a flip-chip package
 - No need to depackage the chip
- Explore attacks feasible under the fault model of the low-cost setup

Contributions

- Characterization of the faults injected by the laser welder
- Demonstration of PFA on a software AES implementation

Laser Welder Demo

- Demonstration of the laser welder (welding two metal parts together)
 - The front panel shows a live camera view of the welding chamber
 - Pressing the trigger fires a laser pulse at the aiming point in the view



Challenges of Using a Laser Welder

- A laser welder is not designed for LFI, so there are some challenges
 - No precise synchronization with the target process
 - Low repetition rate: 1.0–15.0 Hz
 - 50× larger laser spot: less selective injection
 - The chamber is too small for a motorized stage, so scanning is manual

Feature comparison with a professional laser station

	Laser Station 2	MW ST60x (ours)
Price	~€150,000	~\$6,000
Wavelength	1064, 532 nm	1064 nm
Precise synchronization	✓	×
Repetition rate	≤1 kHz	1.0–15.0 Hz
Min. spot size	2 μm	100 μm
Automatic scan	✓	×

Fault Characterization: Items to Verify

Goal of the characterization

- Clarify the fault model of the low-cost setup before designing an attack

Items to verify

- **Feasibility:** Can a laser welder inject faults into a flip-chip device without depackaging?
- **Fault controllability:** Can the success rate and the number of faults be controlled by the laser current?
- **Fault type:** Are the faults transient or persistent?

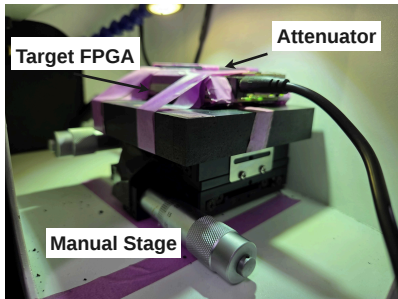
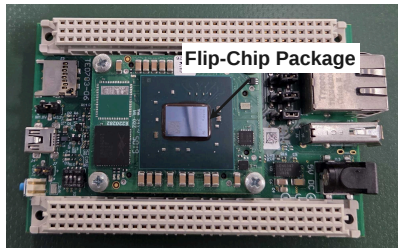
Experimental Setup

Target

- Xilinx Kintex-7 FPGA (28 nm, flip-chip)
- MicroBlaze with 128 KiB BRAM
- Backside illumination, no preparation

Welder modifications (~\$6,000 total)

- **Attenuators:** reduce laser power
- **Manual XY stage:** scan in the small chamber
- **Programmable relay:** trigger pulses from a control PC



Fault Characterization: Procedure

Goal

- Verify and characterize faults in the BRAM data memory of the FPGA

Procedure

- Fill the target memory with a known constant value
- Fire a single laser pulse
- Read back the memory and count the faulty bytes
- Read the memory again to distinguish transient from persistent faults

Repetition

- Repeat the above procedure 200 times for each laser current

Fault Characterization: Laser Current

- **Feasibility: Yes**, our setup successfully injected faults through the backside without depackaging
- **Fault controllability: Yes**, a higher laser current increases the success rate but also the number of faulty bytes
- **Fault type: Persistent**, cleared by a power cycle

Results of 200 shots for each laser current

Laser current	40%	50%	60%	70%
Success rate	0.5%	13.5%	94.5%	100%
Avg. number of faulty bytes per shot	0.2	5.1	66.1	367.0

Fault Model

Capabilities

- Persistent bit flips in the target memory
 - Bidirectional: both $0 \rightarrow 1$ and $1 \rightarrow 0$
- Success rate and number of faults controllable by the laser current

Limitations

- No precise synchronization with the target process
- Multiple bytes corrupted by a single shot
 - Due to the large spot size
- Probabilistic faults, even with a fixed laser position and current
 - Due to machine vibration

End-to-End Evaluation: Threat Model

Threat Model

- An attacker has physical access to the chip and aims to extract the AES-128 key through the chip's standard interface
- Target: a flip-chip package

Equipment

- Only the low-cost laser welder setup
- No high-end laser station and no lab for mechanical or chemical depackaging

Knowledge and access

- No knowledge of the chip's physical details, including laser-sensitive positions
- Black-box access: send chosen plaintexts and obtain the ciphertexts

End-to-End Evaluation: Attack Strategy

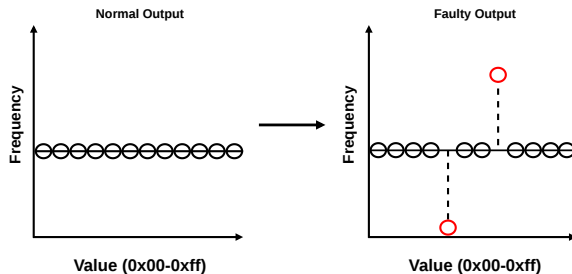
- The attacker needs to choose an attack that works despite the fault-model limitations
- Persistent fault analysis (PFA)¹: target the S-box table in BRAM

Limitation of the fault model	How PFA handles it
No precise synchronization	PFA does not require precise fault timing
Multiple bytes corrupted per shot	PFA works with multiple corrupted entries
Probabilistic faults	Detect faults from ciphertexts and retry
Unknown corrupted entries	No need to know which entries are corrupted

¹Fan Zhang et al. "Persistent Fault Analysis on Block Ciphers". In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2018.3 (2018), pp. 150–172.

Persistent Fault Analysis (PFA)

- PFA exploits faults injected into the S-box table
- A corrupted S-box biases the ciphertext distribution (see figure below)
 - One value never appears, while another appears more often
- The attacker can recover the key from this bias
- By collecting ciphertexts, the attacker can identify the missing value and decide whether PFA is applicable



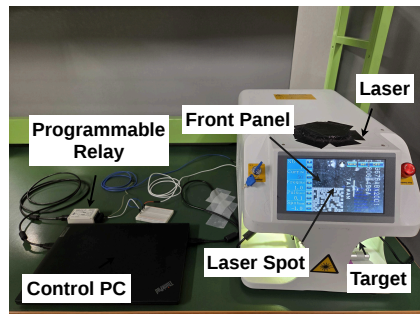
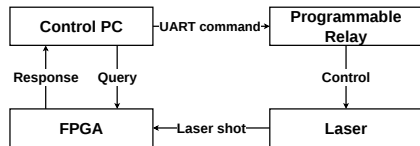
End-to-End Evaluation: Setup & Method

Setup

- Target: software AES-128 on MicroBlaze
 - Uses a 256-byte S-box table
- S-box stored in a dedicated BRAM
 - Other code and data are stored in a separate BRAM
- Laser fixed at a sensitive position (the search method will be explained on the next slide)

Method

- After each shot, send chosen plaintexts to detect a fault
- If a fault is detected, collect 3,600 ciphertexts and recover the key with PFA



End-to-End Evaluation: Sensitivity Search

Goal

- Locate laser-sensitive positions using only black-box access
 - Send plaintexts and obtain the ciphertexts

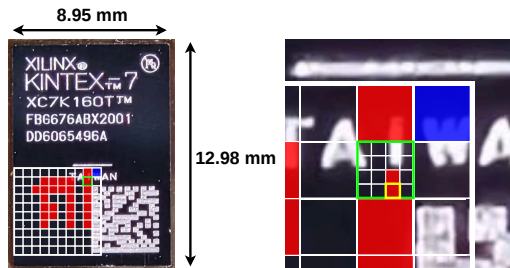
Detection through the encryption interface

- Send chosen plaintexts and check for missing values in the ciphertexts at each laser position

Coarse-to-fine scan with the manual stage

- Coarse scan: 10×10 grid (~ 0.45 mm each), up to 20 shots per subregion
- Fine scan: 4×4 grid (~ 0.11 mm each) inside a sensitive subregion

End-to-End Evaluation: Sensitivity Search Results



Result

- An attacker can find sensitive positions using only black-box access

Legend

- ■ Ciphertext changed, with missing values (usable for PFA)
- ■ Ciphertext changed, without missing values
- ■ Laser position used for key recovery

End-to-End Evaluation: Key Recovery

- We successfully recovered the key in all 17 cases
- λ : number of S-box output values missing due to the fault
- S-box corrupted in 8.5% of the trials ($\lambda \geq 1$)
- Key recovery for $\lambda = 2$ takes longer due to the larger search space
 - More efficient algorithms² exist for $\lambda \geq 3$

Results of 200 shots; average computation time per case for each λ

Number of missing values λ	0	1	2	3	≥ 4
Number of cases	183	10	6	1	0
Computation time	—	0.13 s	796 s	2.79 s	—

²Hadi Soleimany et al. “Practical Multiple Persistent Faults Analysis”. In: *IACR Trans. Cryptogr. Hardw. Embed. Syst.* 2022.1 (2021), pp. 367–390.

Conclusion and Future Work

Conclusion

- Fault injection is feasible without depackaging, even with a low-cost laser welder
- Recovered an AES-128 key from a software implementation on a soft-core processor using PFA

Future work

- Evaluation under a more restricted attacker model
- End-to-end evaluation on a real system